

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

FEB - 1 2019

CLERK'S OFFICE, U.S. DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

UNITED STATES OF AMERICA)
)
 v.) CRIMINAL CASE NO. 1:19-MJ-59
)
 BRANDON THERESA,) Under Seal
)
 Defendant.)

AFFIDAVIT IN SUPPORT OF COMPLAINT AND ARREST WARRANT

I, Jeff Burke being duly sworn, state:

INTRODUCTION

1. I make this affidavit in support of an application for a complaint and arrest warrant for defendant, BRANDON THERESA ("THERESA"). Based on the information detailed below, your affiant submits that there is probable cause to believe that THERESA committed violations of 18 U.S.C. §§ 2261A(2) (cyberstalking).
2. I am a United States Postal Inspector employed by the United States Postal Inspection Service (USPIS) and assigned to the Federal Bureau of Investigation Cyber Task Force (FBI CTF) out of the Washington Field Office. I have been employed by USPIS since May of 2012, including three months of Basic Inspector Training in Potomac, Maryland. Before USPIS, I was employed as a Houston Police Officer where I worked patrol, homicide, and computer crimes investigations. In the course of conducting or participating in criminal investigations, I have been involved in interviewing and debriefing witnesses and informants; conducting physical surveillance; tracing and analyzing internet protocol addresses; tracing and analyzing financial transactions; analyzing telephone pen registers; collecting and analyzing

evidence; and preparing and executing search warrants. I have received organizational sponsored computer training as well as computer training at the SANS institute. I hold several computer forensic certifications including various GIAC certifications, the EnCase Certified Examiner (EnCE), and Certified Computer Examiner (CCE). In addition to my training and certifications, I have been practicing computer forensics since 2006 and have practical experience in the field and have provided expert testimony in both federal and state courts.

3. The facts and information contained in this affidavit are based upon my personal knowledge of the investigation as well as the observations of other law enforcement officers involved in this investigation. All observations that were not personally made by me were related to me by the person(s) who made such observations.

4. The affidavit contains information necessary to support probable cause for this application. The affidavit is not intended to include each and every fact and matter observed by me or known to the government.

PROBABLE CAUSE

Overview of I.S.'s Relationship with THERESA; I.S.'s Attempts to Stop Harassment; and Initiation of Federal Investigation

5. Sometime in or around May of 2014, the victim, I.S., who resided in New York, met THERESA, who resided within the Eastern District of Virginia, online through a mutual friend and interacted with him exclusively via group chat and webcam. Eventually, I.S. and THERESA exchanged phone numbers and their usernames for several instant messaging applications and continued to communicate. The nature of their contact shifted from friendly to romantic.

6. I.S. explained that in March of 2015, she and THERESA first met in person when

THERESA traveled up to New York from Virginia.

7. Soon after their in-person meeting, I.S. noticed unauthorized activity on her online accounts and suspected THERESA's involvement. I.S. confronted THERSEA and, over time, received partial acknowledgements from THERESA that he had, indeed, tampered with her online accounts, contacted her friends, or opened online accounts using her name and other personal information.

8. On June 12, 2016, I.S. filed a complaint with the New York City Police Department (NYPD), stating that THERESA had hacked her Facebook and Twitter accounts and was posting pictures of her. I.S. indicated to the reporting Officer that THERESA was sending emails to her and her parents and making harassing phone calls to both her and her parents.

9. I.S. stated that, in October of 2016, she made it clear to THERESA that she was not interested in a relationship with him and that she did not want to communicate with him further. Despite this, I.S. said that THERESA would continually accuse her of "lying and cheating" on him. I.S. explained that as her frustrations mounted, she asked friends to tell THERESA that she had died and stopped responding to THERESA's attempts to communicate.

10. Federal authorities were alerted to I.S.'s complaints in May 2017 when she and her mother discovered the unauthorized creation of online U.S. Postal Service accounts in their names.

THERESA's Unauthorized Access to I.S.'s Accounts and Creation of New Online Accounts

11. After their first in-person interaction, I.S. discovered that several of her Gmail and Yahoo! emails were appearing as "read" even though she had not opened them. She found this activity strange, but initially dismissed it. When THERESA provided a voluntary statement to law enforcement on December 3, 2018, he admitted that he had accessed I.S.'s email account, but

alleged that he initially had authorization to confirm she was not cheating on him. I.S. denies having provided any such authorization. THERESA admitted to changing the recovery emails in at least one account, however, without permission.

12. Postal business records and business records obtained from Oath Communications and Google indicate that, on several occasions, an Internet Protocol (“IP”) address linked to THERESA was used to log in to I.S.’s online accounts or accounts created without I.S.’s authorization that used I.S.’s personal information. For example, on October 2, 2018, the same IP address was used to access THERESA’s personal email account on the same day it was also used to access an unauthorized usps.com account opened in I.S.’s name without her knowledge or consent, as well as I.S.’s Yahoo email account. Law enforcement confirmed that these IP addresses were issued by a Virtual Private Network (“VPN”) service. VPN services are often used by cybercriminals to obfuscate the IP address information that law enforcement may trace to their real, offline identities. During his interview on December 3, 2018, THERESA admitted to using a VPN service when he accessed unauthorized usps.com accounts.

13. In March of 2015, I.S. logged in to her Gmail account (hereinafter, “I.S.’s Gmail account”) and received a security pop-up indicating that there was an attempted login to her account from an IP address in Virginia. Because I.S. did not know anyone else in Virginia except THERESA, she suspected him of accessing her accounts without her permission and confronted him about the matter. I.S. explained that when she confronted THERESA about the logins, he initially denied it but then alluded to having access and offered to “help her fix it.” After that time, I.S. said that she was again able to access her accounts, but then realized that THERESA had changed the password reset emails to addresses he controlled that were not email addresses I.S. set up or had access to. I.S. believes that, at various times, THERESA obtained

access to a number of her online communications and social media accounts based on changes to her login information that she had not made herself and security notifications she received in connection to her accounts. Records obtained from Oath Communications, which is the parent company of Yahoo!, reveal that someone obtained access to victim I.S.'s Yahoo! email account and changed the recovery email to brandonsoto54@outlook.com and the display name on the email account to "[I.S.'s First Name] Cheater". I.S. confirmed that she never changed her recovery email to brandonsoto54@outlook.com and that she did not authorize that email address to have access to her account.

14. I.S. said that between 2016 and 2017, THERESA not only accessed established accounts that she did not authorize him to access – but also created several new accounts using her identity. I.S. said that THERESA used I.S.'s Yahoo! email account to sign up for things including food deliveries. Grubhub, a food delivery service, provided records indicating that food was ordered – to be paid in cash upon delivery – to I.S.'s residence in November of 2018. During THERESA's voluntary interview with law enforcement, he admitted that he had sent the aforementioned delivery to I.S.'s address using Grubhub.

15. I.S. additionally reported that THERESA contacted her friends and classmates, either pretending to be her, or attempting to elicit information from them about her, and harassed people she knew.

16. The creation of the food delivery accounts and Postal accounts, as well as THERESA's communications with I.S.'s friends and classmates, made I.S. fearful that she was being watched by THERESA all the time.

THERESA's Unauthorized Email to Victim's Professor

17. I.S. discovered that an email was sent on October 21, 2016 from her AOL account

(hereinafter, “I.S.’s AOL email account”) to a college professor containing an attachment that consisted of a provocative picture of I.S. The body of the email contained the text:

This is what happens when people cheat, multiple times, in a relationship. Then proceed to tell the other person to kill themselves and go into hiding so they can’t get arrested for murder. That’s your golden student, [I.S.]. Great artist, great at being two faced, and great at cheating on boyfriends.

I.S. explained during an interview that she did not send the above-referenced email and she did not authorize anyone else to access her email account. During the voluntary interview of THERESA by law enforcement on December 3, 2018, THERESA was shown the above-referenced statement and THERESA said he could have sent it and did send something similar from I.S.’s account, but stated that he did not recall if he used those exact words. During a forensic examination of THERESA’s computer, I.S.’s AOL email account appeared alongside a login URL path “https://my.screenname.aol.com/_cqr/login/login.psp.” in unallocated space, indicating that THERESA had either attempted to – or did – log in to I.S.’s AOL email account during his use of the computer.

18. Federal investigators also learned, through its investigation, that the email had been sent from an IP address corresponding to a Reston, Virginia address. Investigators confirmed, through public records and Virginia Department of Motor Vehicle records, that THERESA resided at a Reston, Virginia address at the time the email was sent. Furthermore, the same IP address where the unauthorized email originated was used to log in to THERESA’s usps.com account, which THERESA confirmed was his during his voluntary interview with law enforcement.

Unauthorized Creation of U.S. Postal Service Informed Delivery Accounts

19. On May 6, 2017, I.S. filed a complaint with the United States Postal Service

(“USPS”), indicating that she believed THERESA was using the USPS Informed Delivery service to intercept photographs of the outside of all of her mail to her home address, because she had started receiving harassing messages from THERESA, in which he described some of the mail she was receiving and stated that he knew where she lived. I.S. believed THERESA engaged in this activity to further place her under surveillance and harass her, because he would periodically confront her about where she lived. I.S. confirmed that she did not create or authorize anyone else to create USPS accounts using her name or address.

20. Informed Delivery is a free service provided by the USPS that allows individuals who have an account at usps.com to receive periodic emails that contain scans or photographs of the outside envelope of all first class mail pieces sent to an address. To obtain such an account, the user also has to confirm that he or she is the person requesting the account and/or that he or she has permission to receive mail at the address associated with the account.

21. Federal authorities reviewed USPS business records and learned that several usps.com accounts associated with I.S.’s address had been created. For instance, on March 18, 2017, a new usps.com account was created in the name of Z.S., I.S.’s mother, who resided at the same address as I.S. Z.S. confirmed that she did not authorize the creation of the usps.com account bearing her name and address. Through its review of lawfully obtained internet subscriber records, law enforcement later determined that the IP address used to create and access the unauthorized USPS account in Z.S.’s name was assigned to THERESA’s residence.

22. On or about May 28, 2017, THERESA and I.S. engaged in a lengthy text message conversation in which THERESA indicated that he understood how to sign up for, and use, the Informed Delivery service.

23. Apart from the USPS account opened in Z.S.’s name, law enforcement discovered

several other unauthorized accounts that had been opened to provide information about mail sent to I.S.'s address. During his voluntary interview with law enforcement on December 3, 2018, THERESA admitted that he had created multiple Informed Delivery accounts using the names and addresses of other people. He also admitted that he had opened several Informed Delivery accounts in order to monitor I.S.'s activities.

24. Law enforcement identified several other unauthorized usps.com accounts opened using the names and personal identifying information of individuals I.S. knew. When these individuals were interviewed by law enforcement, they confirmed they did not create these accounts or authorize someone else to create them. USPS records indicate that the IP addresses from which these unauthorized accounts were created were issued by a VPN service known as privateinternetaccess.com. During his voluntary interview with law enforcement, THERESA admitted to the use of a VPN service, and forensic artifacts on his computers indicated that he was using this VPN service at the time these accounts were created.

25. Forensic evidence discovered on THERESA's laptop, which was seized from his home pursuant to a search warrant on December 3, 2018, indicates that THERESA had logged in to the Informed Delivery accounts of I.S., Z.S., and other individuals I.S. knew, using that computer. As described above, I.S. and Z.S., as well as individuals I.S. knew, did not authorize the creation, or use, of Informed Delivery accounts bearing their personal information.

CONCLUSION

26. Based upon the foregoing, there is probable cause to believe that from approximately March 2015 through approximately November 2018, in the Eastern District of Virginia and elsewhere, THERESA committed violations of 18 U.S.C. §§ 2261A(2) (cyberstalking).



Jeff Burke
Inspector / FBI Task Force Officer
U.S. Postal Inspection Service

Approved by: AUSA Laura Fong

Sworn to and subscribed before me
this 1st day of February 2019 M

Michael S. Nachmanoff
United States Magistrate Judge
Hon. Michael S. Nachmanoff
U.S. Magistrate Judge